IN THE CLAIMS

For the convenience of the Examiner, all pending claims of the present Application are presented below whether or not an amendment has been made. Please amend the claims as follows:

1. **(Currently Amended)** A server comprising:

a communications module operable to receive a dual communication packet from a client over a first channel, the dual communication packet including a header having a client external IP address and a data payload having an encrypted port command having a client internal IP address and a client data port number;

a codec operable to decrypt the encrypted port command;

a translation module operable to retrieve the client external IP address from the header and to generate a modified port command including the external IP address; and

the server operable to establish a second channel based on the modified port command.

2. **(Original)** The server of Claim 1, further comprising a packet filtering server firewall.

3. **(Previously Presented)** The server of Claim 2, further comprising a network address translator associated with the server firewall, the network address translator operable to include a static network address translation entry for each of the client and the server.

4. **(Original)** The server of Claim 1, further comprising a file transfer protocol (FTP) communication module wherein the communication session between the server and the client over the second channel is conducted in secure FTP.

5. **(Previously Presented)** The server of Claim 1, wherein the codec is operable to decrypt based on secure socket layer (SSL) encryption technology.

6. **(Currently Amended)** A client, comprising:

a communications module operable to receive a communication packet from a server over a first channel, the communication packet including a header having a server external IP address and a data payload having an encrypted port command having a server internal IP address and a server data port number;

a codec operable to decrypt the encrypted port command;

a translation module operable to retrieve the server external IP address from the header and to generate a modified port command including the external IP address; and

the server operable to establish a second channel based on the modified port command.

7. **(Original)** The client of Claim 6, further comprising a packet filtering client firewall.

8. **(Previously Presented)** The client of Claim 7, further comprising a network address translator associated with the client firewall, the network address translator operable to include a static network address translation entry for each of the client and the server.

9. **(Previously Presented)** The client of Claim 6, further comprising a file transfer protocol (FTP) communication module wherein a communication session between the server and the client over the second channel is conducted in secure FTP.

10. **(Previously Presented)** The client of Claim 6, wherein the codec is operable to decrypt based on secure socket layer (SSL) encryption technology.

11. **(Currently Amended)** A method for establishing a data socket between first and second peers, comprising:

receiving an IP Packet from the first peer, the IP packet including a header and a port command;

the header including a first peer IP address and the port command including an encrypted second peer IP address;

decrypting ~~decoding~~ the encrypted second peer IP address;

retrieving the first peer IP address from the header;

generating a modified port command including the first peer address in place of the second peer IP address; and

using the modified port command to establish a data socket between the first and second peers.

12. **(Currently Amended)** A method for establishing a transient channel over a non-transient channel, comprising:

receiving an IP packet over the non-transient channel, the IP packet including a header and a port command;

the header including a first peer IP address and the port command including an encrypted second peer IP address;

decrypting ~~decoding~~ the encrypted second peer IP address;

retrieving the first peer IP address from the header;

generating a modified port command including the first peer IP address in place of the second peer IP address; and

using the modified port command to establish the transient channel between a server and a client.

13. **(Previously Presented)** A computer readable medium encoded with a computer program operable to:

receive an IP packet from a first peer, the IP packet including a header and a port command;

the header including a first peer IP address and the port command including an encrypted second peer IP address;

decrypt the encrypted second peer IP address;

retrieve the first peer IP address from the header;

generate a modified port command including the first peer IP address in place of the second peer IP address;

establish a data socket between the first peer and a second peer using the modified port command.

14. **(Currently Amended)** A method for establishing a data socket between a server and a client, comprising:

encrypting ~~encoding~~ a port command including a client internal IP address and a client port number;

generating a dual channel communication packet having a header and a data payload, the header including a server external IP address, server port number, the client internal IP address and the client port number;

the data payload including the encrypted port command;

transmitting the communication packet between the server and the client;

decrypting ~~decoding~~ the encrypted port command;

retrieving a client external IP address from the header;

modifying the decrypted port command by overriding the client internal IP address within the decrypted port command with the client external IP address retrieved from the header; and

establishing a data socket between the server and the client using the modified decrypted port command.

15. **(Original)** The method of Claim 14, further comprising readdressing the client internal IP address within the header with the client external IP address, at a client firewall.

16. **(Previously Presented)** The method of Claim 14, further comprising readdressing the server external IP address within the header with a server internal IP address at a server firewall.

17. **(Currently Amended)** A method for establishing a data socket between a server and a client, comprising:

transmitting a passive command to the server;

encrypting ~~encoding~~ a port command including a server private IP address and a server port number;

creating a dual channel communication packet having a header and a data payload, the header including a client external IP address, client port number, a server internal IP address and the server port number;

the data payload including the encrypted port command;

transmitting the communication packet to the client;

decrypting ~~decoding~~ the encrypted port command;

retrieving a server external IP address from the header;

modifying the decrypted port command by overriding the server internal IP address within the decrypted port command with the server external IP address retrieved from the header; and

establishing a data socket between the server and the client using the modified decrypted port command.

18. **(Previously Presented)** The method of Claim 17, further comprising readdressing the server internal IP address within the header with the server external IP address at a server firewall.

19. **(Previously Presented)** The method of Claim 17, further comprising readdressing the client external IP address in the header with a client internal IP address, at a client firewall.

20. **(Currently Amended)** A method for transferring information over an external network, comprising:

establishing a control channel between a server and a client;

identifying a first end point at a first one of the server and the client, the first end point including a first portion and a second portion;

encrypting ~~encoding~~ the first end point in a secure format;

encapsulating the encrypted first end point in a transmission packet including an address header having the private address of the first end point;

translating the private address in the address header into a public address for transmitting over the external network;

transmitting the transmission packet over the external network in the control channel;

receiving the transmission packet at the other one of the client and the server;

decrypting ~~decoding~~ the encrypted first end point; and

modifying the end point by replacing the first portion in the decrypted end point with the public address in the address header, and establishing a data channel between the client and the server using the modified end point.

21. **(Cancelled)**